Diviseurs Premiers De Suites Recurrentes Lineaires

JEAN PAUL BEZIVIN

Let P be a polynomial with rational integer coefficients. In this paper, we study the rational primes p with the following property: For any linear recurrent sequence of rational integers $U = U_n$ $n \in \mathbb{N}$, with characteristic polynomial P, there is a positive integer n such that $U(n) \equiv 0[p]$. We show, when the polynomial P is irreducible modulo p, that there is a procedure to decide when p satisfy this property. The procedure is connected with a cyclic difference set A depending on p and P.

1. INTRODUCTION ET NOTATIONS

Soit P un polynôme, à coefficients dans $\mathbb{Z}$, de terme constant non nul, de degré s supérieur ou égal à deux. Nous nous proposons d'étudier le problème suivant. Trouver une procédure permettant de décider, si un nombre premier p donné possède la propriété suivante:

Pour toute suite récurrente linéaire, à valeurs dans $\mathbb{Z}$, de polynôme caractéristique P, il existe un terme de cette suite divisible par p. Nous rappelons que si P est le polynôme $a_s X^s + \cdots + a_0$ appartenant à $\mathbb{Z}[X]$, une suite récurrente linéaire $U = U(n)$, $n \in \mathbb{N}$, de polynôme caractéristique P, est une suite (qui sera toujours supposée à valeurs dans $\mathbb{Z}$) vérifiant la relation:

$$a_s U(n+s) + a_{s-1} U(n+s-1) + \cdots + a_0 U(n) = 0, \qquad \forall n \in \mathbb{N}.$$

Dans toute la suite, nous supposerons le polynôme P unitaire, c'est-à-dire $a_s = 1$; ceci n'est pas une restriction, en vertu du lemme de Fatou, (voir [2]). Soit W une suite d'éléments de $\mathbb{Z}$; nous dirons que le nombre premier p est un diviseur de la suite W, s'il existe un élément n de $\mathbb{N}$ tel que p divise $W(n)$. Dans le cas $s = 2$, ce problème a été résolu par divers auteurs (voir [3], [6], et aussi [5] pour des généralisations à des diviseurs non forcément premiers).

Nous aurons besoin de quelques nouvelles notations pour expliciter les résultats du cas $s = 2$.

On pose $P(X) = X^2 + aX + b$, en supposant b non nul, et on définit une suite récurrente linéaire $R = R(n)$, $n \in \mathbb{N}$, de polynôme caractéristique P, à valeurs dans $\mathbb{Z}$, par les valeurs initiales $R(0) = 0$ et $R(1) = 1$. Pour p ne divisant pas le terme constant b du polynôme P, on note $r(p)$ le plus petit entier n strictement positif, tel que p divise $R(n)$. On a alors le résultat suivant:

THEOREME 1 ([3], [6]). *Soit p un nombre premier ne divisant pas le terme constant du polynôme P. Pour que p soit un diviseur de toute suite récurrente linéaire d'ordre 2, à valeurs dans $\mathbb{Z}$, de polynôme caractéristique P, il faut et il suffit que $r(p) = p + 1$.*

On dispose donc dans ce cas d'une méthode pour tester si un nombre premier p ne divisant pas b est un diviseur de toute suite récurrente linéaire, à valeurs dans $\mathbb{Z}$, de polynôme caractéristique P.

On notera que la condition $r(p) = p + 1$ implique que P est irréductible modulo p. Il est d'ailleurs évident que si P est réductible, alors P possède une racine t dans $\mathbb{F}_p - \{0\}$, et une suite $U(n)$ récurrente linéaire, à valeurs dans $\mathbb{Z}$, de polynôme caractéristique P et telle que $U(n) \equiv t^n$ $[p]$ $\forall n$ ne possède pas p pour diviseur. Notre propos est de généraliser le théorème 1 aux suites récurrentes d'ordre supérieur.

0195-6698/030199+06 $02.00/0

Malheureusement, l'énoncé correspondant (théorème 2 ci-dessous), n'est pas aussi simple. Notons toutefois, que dans la mesure où l'on connait un élément primitif de $\mathbb{F}_p s$ sur $\mathbb{F}_p$, et l'ordre réduit du polynôme P modulo p (voir la définition 2), on a aussi une méthode, dans le cas où P est irréductible modulo p, pour décider si p est un diviseur de toute suite récurrente linéaire, à valeurs dans $\mathbb{Z}$, de polynôme caractéristique P. Bien entendu, comme il n'y a qu'un nombre fini de suites récurrentes linéaires, à valeurs dans $\mathbb{F}_p$, de polynôme caractéristique l'image de P dans $\mathbb{F}_p[X]$, on peut aussi étudier chacune de ces suites (qui sont périodiques).

2. Notations et Rappels

Nous rappelons tout d'abord la notion d'ensemble cyclique aux différences.

Definition 1. Soit v un entier non nul, et A une partie de $\mathbb{Z}/v\mathbb{Z}$. On dit que A est un ensemble cyclique aux différences, de type v, k, λ, si A est de cardinal k, et si, pour tout élément non nul c de $\mathbb{Z}/v\mathbb{Z}$, l'équation $a-b=c$ possède exactement λ couples (a, b) solutions dans $A\times A$.

Pour tout ce qui concerne ce sujet, on renvoie à [1]. La notion d'ensemble cyclique aux différences sera fondamentale dans tout ce qui suit.

Soit P un polynôme de degré s supérieur ou égal à 2, unitaire et à coefficients dans $\mathbb{Z}$.

On supposera, dans tout ce qui suit, que le polynôme P est irréductible dans $\mathbb{Z}[X]$.

On note alors $I(P)$ l'ensemble des nombres premiers p tels que l'image de P dans $\mathbb{F}_p[X]$ (image que nous noterons toujours P, conformément à l'usage) soit irréductible. Pour $s=2$ ou 3, on sait que $I(P)$ est un ensemble infini; pour $s\geqslant 4$, $I(P)$ peut être vide (voir [4], p. 139, ex 5 et 6). Pour p appartenant à $I(P)$, on note L un corps de rupture de l'image de P dans $\mathbb{F}_p[X]$, et α_i, $1\leqslant i\leqslant s$, les racines de P dans L.

Soit G le sous-groupe multiplicatif de L^* engendré par les quotients des racines de P dans L.

Nous noterons $h(p, P)$ (et pour simplifier $h(p)$, quand il n'y aura pas de confusion possible) l'ordre du groupe G.

Definition 2. L'ordre $h(p, P)$ du groupe G sera appelé l'ordre réduit du polynôme P modulo p.

L'ensemble des suites récurrentes linéaires, à valeurs dans $\mathbb{Z}$, de polynôme caractéristique P, sera noté $S(P)$. Pour p élément de $I(P)$, nous noterons de même $S(p, P)$ l'ensemble des suites récurrentes linéaires, à valeurs dans $\mathbb{F}_p$, de polynôme caractéristique $P\in\mathbb{F}_p[X]$.

Enfin, nous noterons $D(P)$ l'ensemble des nombres premiers p de $I(P)$, tels que p soit un diviseur de toute suite de $S(P)$. On voit immédiatement que p appartient à $D(P)$, si et seulement si toute suite de $S(p, P)$ prend au moins une fois la valeur zéro.

Nous dirons qu'un élément p de $D(P)$ est un diviseur universel de P.

3. Formulation des Resultats

Nous allons démontrer les résultats suivants:

Theoreme 2. *Soit P un polynôme unitaire, à coefficients dans $\mathbb{Z}$, de degré $s\geqslant 2$, irréductible, et p tel que P soit encore irréductible modulo p. On définit u et v par les relations: $uh(p)=v=1+p+\cdots p^{s-1}$. Il existe un ensemble cyclique aux différences A, de paramètres*

v, $k=(p^{s-1}-1)/(p-1)$, $\lambda=(p^{s-2}-1)/(p-1)$ *ne dépendant que du nombre premier* p *et de l'entier* s, *tel que* (a) *et* (b) *soient équivalentes*:
(a) *toute suite récurrente linéaire à valeurs dans* $\mathbb{Z}$ *admettant* P *comme polynôme caractéristique possède un zéro modulo* p;
(b) *la restriction à* A *de l'application canonique* φ *de* $\mathbb{Z}/v\mathbb{Z}$ *dans* $\mathbb{Z}/u\mathbb{Z}$ *est surjective.*

THEOREME 3. *Sous les mêmes hypothèses que dans le théorème* 2 *on a, pour* p *appartenant à* $I(P)$ *et* $s\geqslant 3$, *les résultats suivants*:
(a) $h(p)\geqslant[p^s+(p-1)^2/4]^{1/2}-(p-1)/2$ *entraîne que toute suite récurrente linéaire à valeurs dans* $\mathbb{Z}$ *admettant* P *comme polynôme caractéristique possède un zéro modulo* p;
(b) *si toute suite récurrente linéaire à valeurs dans* $\mathbb{Z}$ *admettant* P *comme polynôme caractéristique possède un zéro modulo* p, *alors on a* $h(p)\geqslant p+1+\sqrt{p}$ *pour* $s=3$ *et* $h(p)\geqslant p+1$ *pour* $s\geqslant 4$.

Dans le cas $s=3$, des résultats de même nature que ceux du théorème 3 ont été démontrés par Ward sous la forme que voici:

THEOREME 4 (Ward, [7]). *Sous les hypothèses du théorème* 2, *et pour* $s=3$, *chacune des conditions* (a), (b) *ou* (c) *suivantes entraîne que toute suite recurrente linéaire à valeurs dans* $\mathbb{Z}$ *admettant* P *comme polynôme caractéristique possède un zéro modulo* p.
(a) $h(p)=1+p+p^2$;
(b) $3\mid 1+p+p^2$ *et* $h(p)=(1+p+p^2)/3$;
(c) $7\mid 1+p+p^2$ *et* $h(p)=(1+p+p^2)/7$.

4. Lemmes Preliminaires

Dans tout ce qui suit, p est un élément de $I(P)$ (c'est à dire P est irréductible modulo p).

LEMME 1. (a) *L'ordre réduit* $h(p)$, *défini plus haut, est le plus petit entier strictement positif* n *tel que la condition suivante soit réalisée: Il existe* a *dans* $\mathbb{F}_p$, *tel que* P *divise le polynôme* X^n-a *dans* $\mathbb{F}_p$.
(b) *L'ordre réduit divise* $v=1+p+\cdots+p^{s-1}=(p^s-1)/(p-1)$.

PREUVE. (a) pour tout couple (i,j) d'entiers compris entre 1 et s, on a $\alpha_i^{h(p)}=\alpha_j^{h(p)}$ d'après la définition de $h(p)$. Soit a la valeur commune des $\alpha_i^{h(p)}$. L'élément a est dans $\mathbb{F}_p$ et il est clair que P divise $X^{h(p)}-a$. Réciproquement, si P divise X^n-a, alors n est un multiple de $h(p)$.
(b) Soit α_i une racine de P dans L. La norme de α_i sur $\mathbb{F}_p$ est $\alpha_i^{1+p+\cdots+p^{s-1}}=\alpha_i^v$ et appartient donc à $\mathbb{F}_p$; il en résulte que $h(p)$ divise v.

DEFINITION 3. Soit θ un élément de L^*. On dit que θ est une racine pseudo-primitive si l'image de θ dans le groupe $L^*/\mathbb{F}_p^*$ en est un générateur.

LEMME 2. *Soit* θ *une racine pseudo-primitive de* L^*, *et* Q *son polynôme minimal. Alors l'ordre réduit de* Q *est* $v=1+p+\cdots+p^{s-1}$. *Soit* W *la suite récurrente linéaire d'éléments de* $\mathbb{F}_p$, *de polynôme caractéristique* Q *définie par* $W(n)=\sum_1^s\theta_i^n$ *où les* θ_i, $1\leqslant i\leqslant s$ *sont les racines de* Q. *Toute suite* U *de* $S(p,P)$ *est une sous-suite de* W *dans le sens suivant: Il existe* b *appartenant à* $\mathbb{F}_p$, a *appartenant à* $\mathbb{F}_p^*$, c *dans* $\mathbb{N}^*$ *et* d *dans* $\mathbb{Z}$, *tels que, pour tout* n *dans* $\mathbb{Z}$ *on ait* $U(n)=ba^nW(cn+d)$.

PREUVE. La première assertion est évidente, puisque l'ordre du groupe $L^*/\mathbb{F}_p^*$ est $1+p+\cdots+p^{s-1}=v$.

Soit U appartenant à $S(p,P)$. On peut écrire dans L, $U(n)=\sum_{i=1}^{s}\lambda_i\alpha_i^n$, les λ_i $1\leqslant i\leqslant s$ étant des élements de L. Puisque $\theta=\theta_1$ est une racine pseudo-primitive, on peut écrire $\alpha_1=a\theta_1^c$ et $\lambda_1=b\theta_1^d$, avec c élément de $\mathbb{N}^*$, a et b dans $\mathbb{F}_p$ et d dans $\mathbb{Z}$.

Il résulte alors du fait que U est à valeurs dans $\mathbb{F}_p$, que l'on peut supposer, pour tout i compris entre 1 et s:

$\alpha_i=a\theta_i^c$ et $\lambda_i=b\theta_i^d$. Par conséquent, on a:

$U(n)=\sum_{i=1}^{s} ba^n\theta_i^{cn+d}=ba^nW(cn+d)$, ce qui démontre le lemme 2.

LEMME 3. *On se place dans les conditions du lemme* 2, *et on note u le plus grand commun diviseur de c et* $v=(p^s-1)/(p-1)$. *On a alors la relation* $uh(p)=v$.

PREUVE. On a $\alpha_1=a\theta^c=a\theta_1^c$, en utilisant les notations du lemme précédent. L'ordre de l'image de α_1 dans le groupe $L^*/\mathbb{F}_p^*$ est alors égal à l'ordre dans $L^*/\mathbb{F}_p^*$ de θ^c, et puisque θ est une racine pseudo-primitive, l'ordre de θ^c est égal à v divisé par le PGCD de c et de v. D'où le résultat, puisque l'ordre de α_1 dans $L^*/\mathbb{F}_p^*$ est aussi l'ordre réduit modulo p du polynôme P.

LEMME 4. *Soit* θ *une racine pseudo-primitive, et W la suite récurrente linéaire, à valeurs dans* $\mathbb{F}_p$, *définie dans le lemme* 2 *précédent. On note* $B=\{n\in\mathbb{Z}\mid W(n)=0\}$. *Alors l'image de B dans* $\mathbb{Z}/v\mathbb{Z}$ *est un ensemble cyclique aux différences, de paramètres* $v=(p^s-1)/(p-1)$, $k=(p^{s-1}-1)/(p-1)$, $\lambda=(p^{s-2}-1)/(p-1)$. *De plus, si b appartient à B, alors, pour tout m dans* $\mathbb{Z}$, $b+mv$ *appartient à B.*

PREUVE. La première assertion se déduit de [1], chapitre V, page 103, on prend pour forme linéaire la trace; voir aussi la remarque du bas de la page 103, pour le cas d'une racine pseudo-primitive au lieu d'une racine primitive. La deuxième assertion est évidente.

LEMME 5. *Soit A un ensemble cyclique aux différences, de paramètres v, k,* λ, *et u diviseur de v. On note, pour i appartenant à* $\mathbb{Z}/u\mathbb{Z}$, b_i *le cardinal de l'ensemble des éléments a de A tels que* $\varphi(a)=i$, *où* φ *est la surjection canonique de* $\mathbb{Z}/v\mathbb{Z}$ *sur* $\mathbb{Z}/u\mathbb{Z}$. *On a alors les trois relations suivantes*:

(a) $\sum b_i=k$;

(b) $\sum b_i^2=k-\lambda+v/u$;

(c) $\sum b_ib_{i-j}=\lambda v/u\ (j\in\mathbb{Z}/u\mathbb{Z}, j\neq 0)$.

où les trois sommations ont lieu sur les indices i appartenant à $\mathbb{Z}/u\mathbb{Z}$.

PREUVE. Voir [1], page 24.

5. PREUVE DES THEOREMES 2 ET 3

PREUVE DU THÉORÈME 2. D'après le lemme 2, et en utilisant les notations qui y sont introduites, toute suite U de $S(P)$ admet p pour diviseur, pour p appartenant à $I(P)$, si et seulement si, pour tout élément d de $\mathbb{Z}$, il existe un entier n tel que $cn+d$ appartienne à l'ensemble B des zéros de la suite W introduite dans le lemme 2.

Autrement dit, il est nécessaire et suffisant que B rencontre toute classe modulo c.

Nous allons prendre pour l'ensemble A du théorème 2 l'image de B dans $\mathbb{Z}/v\mathbb{Z}$.

D'après les propriétés de B (cf. lemme 4) on voit donc qu'il suffit, pour démontrer le théorème 2, de montrer que la condition 'B rencontre toute classe modulo u' équivaut à: 'B rencontre toute classe modulo c'. (On rappelle que u est le plus grand commun

diviseur de c et v). Si B rencontre toute classe modulo c, il est clair que B rencontre toute classe modulo u, puisque u divise c. Réciproquement, supposons que B rencontre toute classe modulo u. On pose $ut = c$ et $uq = v$, avec t et q premiers entre eux.

Soit x appartenant à $\mathbb{Z}$. Il existe b_1 appartenant à B tel que $b_1 = x + ku$; pour tout m dans $\mathbb{Z}$, on sait d'après le lemme 4 que $b_1 + mv$ appartient à B. On va donc chercher m dans $\mathbb{Z}$ tel que $b = b_1 + mv$ soit congru à x modulo c; ceci équivaut à trouver m tel que $mv + ku$ soit divisible par c, ou encore à trouver m tel que $mq + k$ soit divisible par t, et l'existence d'un tel m est évidente puisque t et q sont premiers entre eux, et ceci termine la démonstration du théorème 2.

On peut formuler de façon légèrement différente le théorème 2, en introduisant, pour chaque nombre premier p et chaque entier s supérieur ou égal à deux, un ensemble cyclique aux différences $A(p, s)$, de paramètres $(p^s - 1)/(p - 1), (p^{s-1} - 1)/(p - 1), (p^{s-2} - 1)/(p - 1)$, provenant de l'extension de degré s de $\mathbb{F}_p$, en se fixant une fois pour toute une racine pseudo-primitive de $\mathbb{F}_{p^s}$ (par exemple une racine primitive).

On note alors $D(p, s)$ l'ensemble des diviseurs h de $v = (p^s - 1)/(p - 1)$ tels que si $v = hu$, l'image de $A(p, s)$ dans $\mathbb{Z}/u\mathbb{Z}$ soit $\mathbb{Z}/u\mathbb{Z}$ tout entier par l'application canonique de $\mathbb{Z}/v\mathbb{Z}$ dans $\mathbb{Z}/u\mathbb{Z}$.

THEOREME 2'. *Soit P un polynôme unitaire, à coefficients dans $\mathbb{Z}$, de degré $s \geqslant 2$, irréductible dans $\mathbb{Z}[X]$. Soit p un nombre premier tel que P soit irréductible modulo p. Alors p est un diviseur universel de P, si et seulement si l'ordre réduit de P modulo p appartient à $D(p, s)$.*

On peut regarder plus précisément ce qui se passe pour $s = 2$ et $s = 3$. Dans les deux cas, on voit facilement qu'il est nécessaire, pour que p divise toute suite récurrente linéaire à valeurs dans $\mathbb{Z}$ de polynôme caractéristique P, que P soit irréductible modulo p. (On suppose que p ne divise pas le terme constant du polynôme P; voir l'argument suivant l'énoncé du théorème 1).

Dans le cas $s = 2$, on voit que $v = p + 1$, $k = 1$, $\lambda = 0$. Donc l'ensemble $A(p, 2)$ a un seul élément, et par conséquent, pour que la restriction de l'application canonique de $\mathbb{Z}/(p + 1)\mathbb{Z}$ dans $\mathbb{Z}/u\mathbb{Z}$ à $A(p, 2)$ soit surjective, il est nécessaire et suffisant que $u = 1$; on retrouve donc le théorème 1.

Dans le cas $s = 3$, un phénomène intéressant se produit: il se peut que $v = 1 + p + p^2$ soit premier, ceci se réalise pour $p = 2, 3, 5, 17, 41, \ldots$ etc. Il semble que de telles valeurs de p soient assez nombreuses. Il est clair que dans ce cas $D(p, 3)$ est réduit à $\{v\}$, et qu'une condition nécessaire et suffisante pour que le nombre premier p divise toute suite récurrente linéaire à valeurs dans $\mathbb{Z}$, de polynôme caractéristique P, est que P soit irréductible modulo p.

Pour toute valeur de s, le corollaire suivant au théorème 2 est d'ailleurs évident:

COROLLAIRE. *Soit P un polynôme unitaire de degré $s \geqslant 2$, à coefficients dans $\mathbb{Z}$, et p un nombre premier tel que P soit irréductible modulo p. Alors, si l'ordre réduit de P modulo p est égal à $v = 1 + p + \cdots + p^{s-1}$, toute suite récurrente linéaire à valeurs dans $\mathbb{Z}$, admettant P comme polynôme caractéristique, possède un zéro modulo p.*

Le théorème 1 dit que pour $s = 2$, la condition $h(p) = v$ est nécessaire et suffisante pour que p appartienne à $D(P)$. Dans le cas général, la situation est moins simple, comme le montre le théorème 3 dont nous allons maintenant donner la preuve.

PREUVE DU THÉORÈME 3. On suppose $s \geqslant 3$, soit u un diviseur de $v = 1 + p + \cdots + p^{s-1}$, et h tel que $uh = v$. Nous utilisons les notations du lemme 5. Il faut tout d'abord montrer

que si h est plus grand que $[p^s+(p-1)^2/4]^{1/2}-(p-1)/2$, on a $b_i \neq 0$ pour tout i dans $\mathbb{Z}/u\mathbb{Z}$. Soit $S=\sum (pb_i-h)^2$, la sommation étant faite sur les indices i dans $\mathbb{Z}/u\mathbb{Z}$. A l'aide des relations (a) et (b) du lemme 5, on trouve:

$$S=p^s-(p-1)h.$$

On raisonne alors par l'absurde, en supposant qu'il existe un indice i_0 tel que $b_{i_0}=0$. On a alors:

$$h^2=(pb_{i_0}-h)^2 \leq S=p^s-(p-1)h,$$

d'où $h^2+(p-1)h \leq p^s$, et la conclusion cherchée en résulte. Supposons maintenant $b_i \neq 0$ pour tout i dans $\mathbb{Z}/u\mathbb{Z}$. On peut alors écrire $b_i=1+c_i$ avec c_i appartenant à $\mathbb{N}$. On a alors: $\sum (1+c_i)=k$, et pour j dans $\mathbb{Z}/u\mathbb{Z}$, $j \neq 0$, $\sum (1+c_i)(1+c_{i-j})=\lambda v/u=\lambda h$, les sommations étant faites sur les indices i dans $\mathbb{Z}/u\mathbb{Z}$.

On en tire $\sum c_i=k-u$ et $\Sigma c_i c_{i-j}=\lambda h-2k+u$; la quantité $\lambda h-2k+u$ est donc positive ou nulle.

Ceci équivaut à $(p^{s-2}-1)h^2-2(p^{s-1}-1)h+p^s-1$ positive ou nulle, d'où:

$$\left(h-\frac{p^{s-1}-1}{p^{s-2}-1}\right)^2 \geq (p-1)^2\frac{p^{s-2}}{(p^{s-2}-1)^2}. \qquad (*)$$

Il est d'autre part immédiat que $u \leq \text{card}\,(A)=k$, puisque la restriction de l'application canonique de $\mathbb{Z}/v\mathbb{Z}$ sur $\mathbb{Z}/u\mathbb{Z}$ à A est surjective. Donc $h \geq (p^s-1)/(p^{s-1}-1)=p+(p-1)/(p^{s-1}-1)$; pour $s \geq 3$, on a donc $h \geq p+1$. D'autre part pour $s \geq 3$, $p+1 \geq (p^{s-1}-1)/(p^{s-2}-1)$ et $(*)$ implique alors

$$h \geq \frac{p^{s-1}-1}{p^{s-2}-1}+(p-1)\frac{p^{(s-2)/2}}{p^{s-2}-1}.$$

Pour $s=3$, on trouve $h \geq p+1+\sqrt{p}$; pour $s \geq 4$, on ne trouve pas mieux que l'inégalité $h \geq p+1$ déjà vue.

L'auteur remercie J. Berstel et les référées pour d'intéressantes suggestions de présentation.

References

1. L. Baumert, *Cyclic Difference Sets*, Lecture Notes 182, Springer-Verlag, Heidelberg, 1971.
2. B. Benzaghou, Algèbre de Hadamard, *Bull. Soc. Math. France* **98** (1969), 209-252.
3. P. Catlin, On the divisors of second order recurrence, *Fibonnacci Quarterly* **12** (1974), 175-179.
4. G. J. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.
5. P. Kiss and Bui Minh Phong, Divisibility properties of second order recurrence, *Publicationes Mathematicae* **26** (1979), 187-197.
6. R. R. Laxton, On groups of linear recurrence, *Duke Math. Journal* **36** (1969), 721-736.
7. Ward, The distribution of residues in a sequence satisfying a linear recursion relation, *Trans. Amer. Math. Soc.* **33** (1931), 166-190.

Received 12 March 1984

JEAN-PAUL BEZIVIN
Université Pierre et Marie Curie, Mathématiques,
Tour 45-46, 5ème étage, 4 place Jussieu, 75005 Paris, France